メディア フロー分析の設定

この章には、メディア ソリューション向けのシスコの IP ファブリックのメディア フロー分析に関する情報が含まれています。

RTP フロー モニタリング

リアルタイム トランスポート プロトコル（RTP）は、IP ネットワークを介して音声とビデオをお届けするネットワーク プロトコルです。ストリーミング メディアのエンド ツー エンドのリアルタイム転送用に設計されています。このプロトコルは、IP ネットワークでの UDP 送信中に一般的なジッタ補正とパケット損失の検出のための機能を提供します。

RTP フロー モニタリングは、スイッチ上の RTP フローをキャッシュし、RTP フレームの損失を示す RTP シーケンス番号のギャップを検出します。この情報は、損失が発生している場所を特定するのに役立ち、ハードウェア リソースをより適切に計画できるようになります。

RTP フロー モニタリングの注意事項と制限事項

次の注意事項と制限事項は RTP フロー モニタリングに適用されます。

- Cisco Nexus 9300-FX および 9300-FX2 プラットフォーム スイッチは RTP フロー モニタリングをサポートします。

  さらに、Cisco NX-OS 9.3(6) 以降、Cisco Nexus 9300-GX プラットフォーム スイッチは RTP フロー モニタリングをサポートします。

- RTP フロー モニタリングが最初の ACL で設定され、別の ACL に変更された場合は、コマンドの `no flow rtp` 形式で RTP 設定を削除してから、目的の ACL で再度設定する必要があります。

- RTP フロー モニタリング用に UDF を設定した後、スイッチを再起動する必要があります。
- RTP フロー モニタリング UDF は 1 つだけ設定できます。
- RTP フロー モニタリング UDF は、最初の UDF である必要があります。
- NetFlow と RTP フロー モニタリングは、スイッチ上で共存できません。

RTP フロー モニタリングの設定

Cisco Nexus 9300-FX および 9300-FX2 スイッチの RTP フロー モニタリングを設定できます。

さらに、Cisco NX-OS 9.3(6) 以降、Cisco Nexus 9300-GX プラットフォーム スイッチの RTP フロー モニタリングを設定できます。

始める前に

udf netflow_rtp netflow-rtp コマンドを使用して RTP フロー モニタリングの UDF を有効にし、実行コンフィギュレーションをスタートアップにコピーして、スイッチを再起動します。RTP フロー モニタリング UDF が最初の UDF であることを確認してください。

手順の概要

1. **configure terminal**
2. [**no**] **feature netflow**
3. （任意） **ip access-list** *acl*
4. [**no**] {**ip** | **ipv6**} **flow rtp** [*acl*]

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル設定モードを開始します。

ステップ 2	[**no**] **feature netflow** 例： `switch(config)# feature netflow`	スイッチ上で RTP フロー モニタリングをグローバルに有効にします。

ステップ 3	（任意） **ip access-list** *acl*
	例：
	`ip access-list ipv4-test-acl`
	`  10 permit ip any 224.0.1.39/32`
	`  20 permit ip any 224.0.1.40/32`
		特定のトラフィックをフィルタリングするように ACL ポリシーを設定します。

	コマンドまたはアクション	目的

ステップ 4	[**no**] {**ip** | **ipv6**} **flow rtp** [*acl*]
	例：
	`switch(config)# ip flow rtp`
		IPv4 または IPv6 フローの RTP フロー モニタリングを有効にします。
		• このコマンドは、システム全体のアクセス コントロール リスト (ACL) を作成して、16384 ～ 32767 の UDP ポート範囲をフィルタリングします。この範囲は、RTP トラフィックの RFC 標準 UDP ポート範囲です。
		（注） この **ignore routable** コマンドは、マルチキャスト トラフィックをフィルタリングします。
		`switch(config)# show ip access-list`
		`IP access list nfm-rtp-ipv4-acl`
		`ignore routable`
		`10 permit udp any any range 16384 32767`
		• （注） コマンドで ACL を指定すると、指定した ACL に一致するトラフィックだけが RTP フローとして報告されます。
		`switch(config)# ip flow rtp ipv4-test-acl`

RTP フローとエラーの表示

RTP フローとエラーを表示するには、次のいずれかのタスクを実行します。

show flow rtp details	すべての IPv4 および IPv6 RTP フローを表示します。
show flow rtp details {**ipv4** | **ipv6**}	IPv4 または IPv6 RTP フローを表示します。

show flow rtp errors active	現在損失が発生しているすべての RTP フローの詳細を表示します (過去 10 秒以内の少なくとも 1 つの更新間隔でパケット損失が検出された場合)。アクティブな損失ウィンドウの損失統計も表示されます。損失ウィンドウはまだアクティブであると見なされるため、損失の終了時刻は「N/A」と表示されます。
show flow rtp errors history	過去 1000 件の過去の損失ウィンドウの詳細を (新しい順に) 表示し、それぞれのフローの詳細を表示します。

次の例は、**show flow rtp details** コマンドのサンプル出力を示しています。

```
RTP Flow timeout is 1440 minutes
IPV4 Entries
SIP      DIP      BD ID S-Port D-Port Intf/Vlan Name  Packet Count BytesPerSec  FlowStart
50.1.1.2 20.1.1.2 4151  16385  17999  Ethernet1/49/1  269207033    594468000    00:21:16
 PST Apr 07 2019
20.1.1.2 50.1.1.2 4100  16385  18999  port-channel500 2844253      199000       00:21:59
 PST Apr 07 2019

IPv6 Entries
SIP         DIP    BD ID S-Port D-Port Intf/Vlan Name   Packet Count BytesPerSec FlowStart
20::2        50::2  4100  30000  31999  port-channel500  2820074      199000      00:22:04
 PST Apr 07 2019
50::2        20::2  4151  30000  31999  Ethernet1/49/1   3058232      199000      00:21:16
 PST Apr 07 2019
```

次の例は、**show flow rtp errors active** コマンドのサンプル出力を示しています。

```
RTP Flow timeout is 1440 minutes
IPV4 Entries
SIP             DIP             BD ID   S-Port  D-Port  Intf/Vlan Name      Packet Count
     BytesPerSec  FlowStart                Packet Loss Loss Start                Loss
End
30.30.1.2       20.20.1.2       4197    30000   20392   Ethernet1/98        200993031
      10935633     20:23:15 UTC May 30 2019  1558        03:48:32 UTC May 31 2019  N/A
20.20.1.2       30.30.1.2       4196    30000   20392   Ethernet1/97        204288988
      11114959     20:23:15 UTC May 30 2019  222         03:48:30 UTC May 31 2019  N/A
```

（注） RTP フローが「アクティブ エラー」状態になると、次の syslog メッセージが表示されます。

```
%NFM-1-RTP_FLOW_ERROR_DETECTED: Flow SIP: 30.30.1.2 DIP: 20.20.1.2 Interface: Ethernet1/98
 loss detected
```

次の例は、**show flow rtp errors history** コマンドのサンプル出力を示しています。

```
RTP Flow timeout is 1440 minutes
IPV4 Entries
SIP             DIP             BD ID   S-Port  D-Port  Intf/Vlan Name      Packet Count
     BytesPerSec  FlowStart                Packet Loss Loss Start                Loss
End
20.20.1.2       30.30.1.2       4196    30000   20392   Ethernet1/97        204187441
      11122753     20:23:15 UTC May 30 2019  2061        03:47:57 UTC May 31 2019
03:47:57 UTC May 31 2019
30.30.1.2       20.20.1.2       4197    30000   20392   Ethernet1/98        199495510
      10937237     20:23:15 UTC May 30 2019  1882        03:45:06 UTC May 31 2019
03:45:06 UTC May 31 2019
20.20.1.2       30.30.1.2       4196    30000   20392   Ethernet1/97        202753418
      11116269     20:23:15 UTC May 30 2019  4976        03:45:05 UTC May 31 2019
03:45:05 UTC May 31 2019
20.20.1.2       30.30.1.2       4196    30000   20392   Ethernet1/97        202630465
      11123369     20:23:15 UTC May 30 2019  2139        03:44:32 UTC May 31 2019
03:44:32 UTC May 31 2019
30.30.1.2       20.20.1.2       4197    30000   20392   Ethernet1/98        197973969
      10938370     20:23:15 UTC May 30 2019  1854        03:41:41 UTC May 31 2019
03:41:41 UTC May 31 2019
```

（注） RTP フローが「アクティブ エラー」状態でなくなると、次の syslog メッセージが表示されます。

```
%NFM-1-RTP_FLOW_ERROR_STOP: Flow SIP: 30.30.1.2 DIP: 20.20.1.2 Interface: Ethernet1/98
loss no longer detected
```

RTP フローのクリアリング

RTP フローをクリアするには、次のタスクのいずれかを実行します。

clear flow rtp detail	すべての RTP フローと損失履歴をクリアします。
clear flow rtp detail {**ipv4** | **ipv6**}	IPv4 または IPv6 RTP フローと損失履歴をクリアします。

[**no**] **flow rtp timeout** *value* 例： `switch(config)# flow rtp timeout 100`	**show rtp details**, **show flow rtp errors active** および **show flow rtp errors history** テーブルから非アクティブな RTP フローをクリアします。 デフォルト値は 1440 分（24 時間）で、範囲は 0 ～ 1440 分です。値 0 は、RTP フローがクリアされないようにします。 （注） このコマンドは、アクティブな RTP フローをクリアしません。